Nattan MAISONNEUVE–FLEURY
BTS SIO 1
Groupe B

02/10/2025

Compte Rendu - Cyber

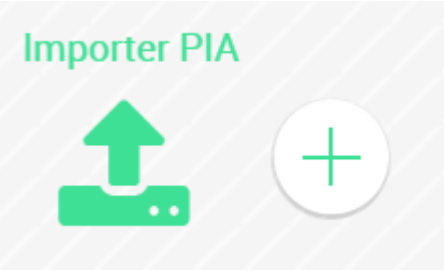
Sommaire :

Introduction :

Dans ce TP nous allons découvrir comment vérifier comment est sécurisée l'entreprise et comment faire une expertise afin de savoir quoi améliorer. De plus, nous verrons l'utilisation des données à caractères personnel et leur traitement.

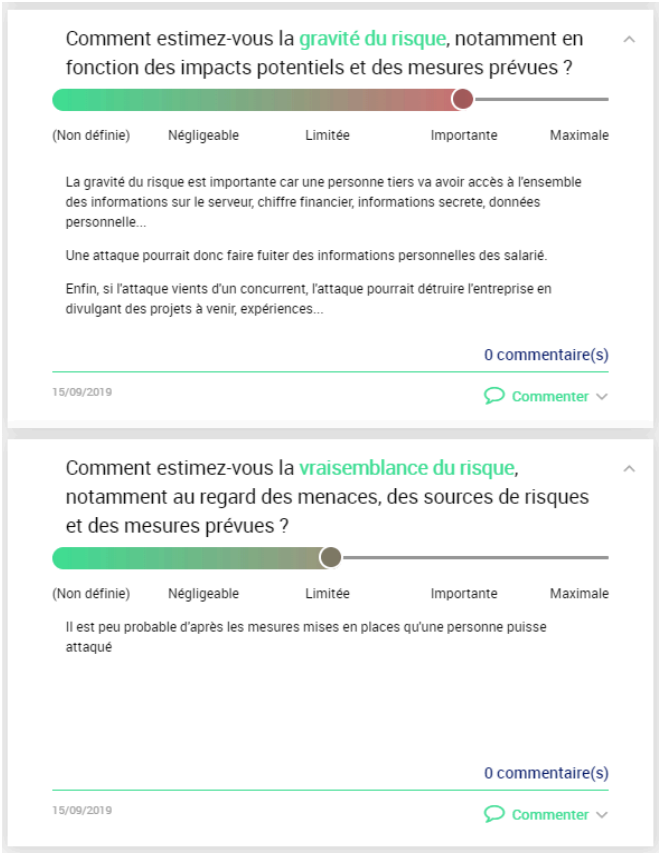
Exercices 1 :

1) Importation du travail réalisé par M.Grospire dans l'application PIA en cliquant sur ce bouton :

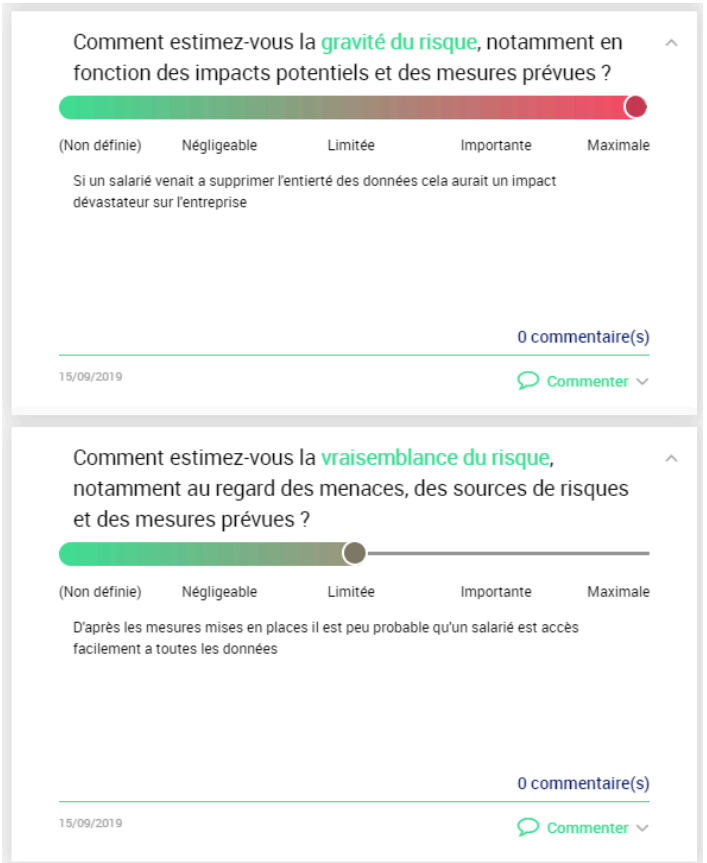


Le travail de M.Grospire ce télécharge dans l'application :

2) Pour le risque d'**accès illégitime à des données** :

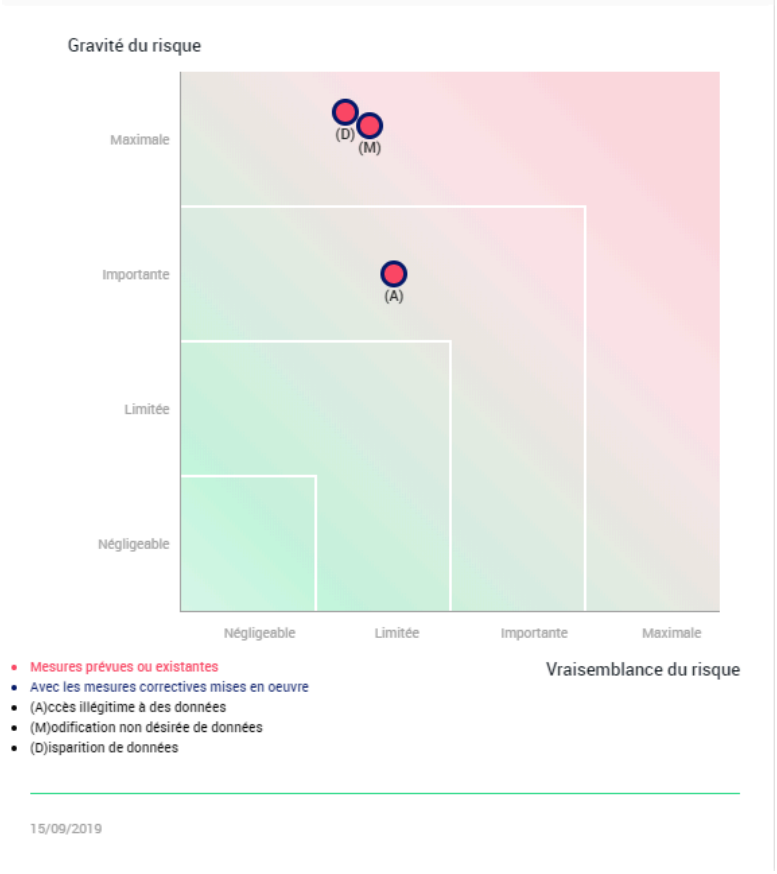


Pour le risque **modification non désiré de donnée** :

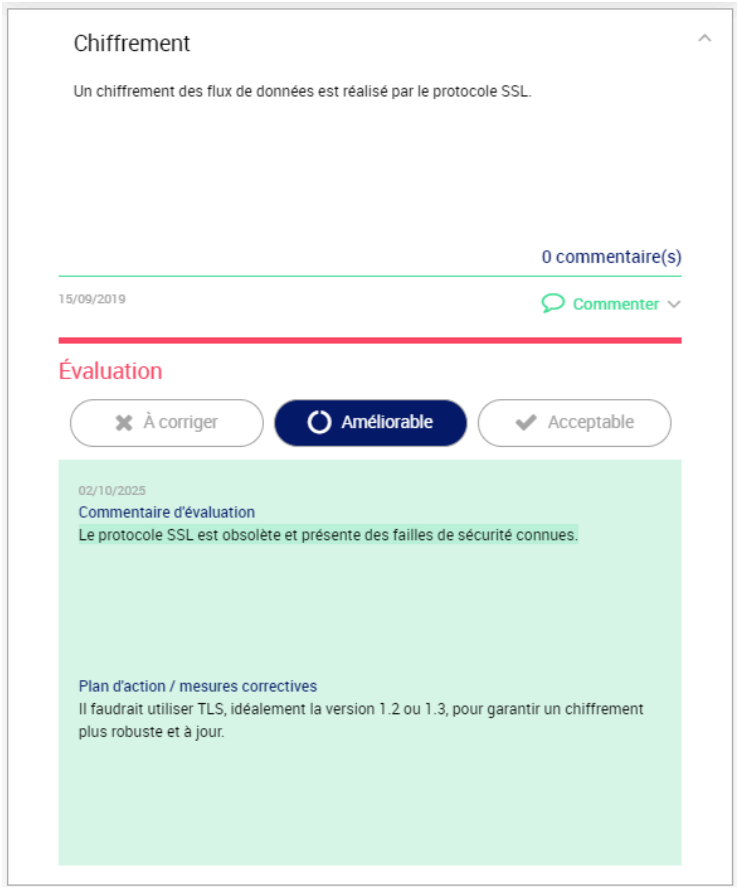


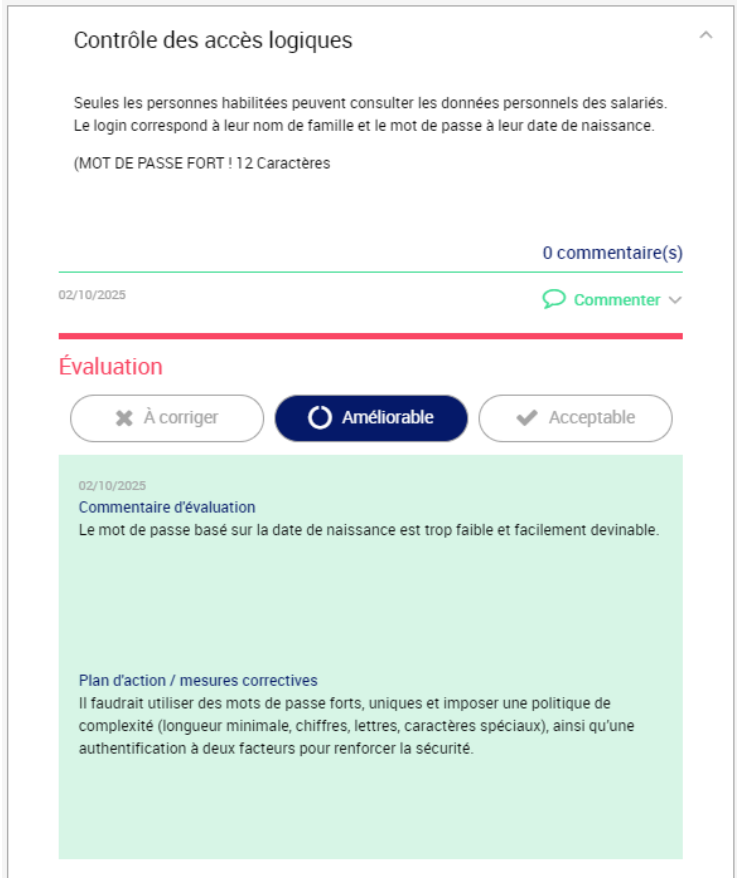
Pour le risque **disparition de données**

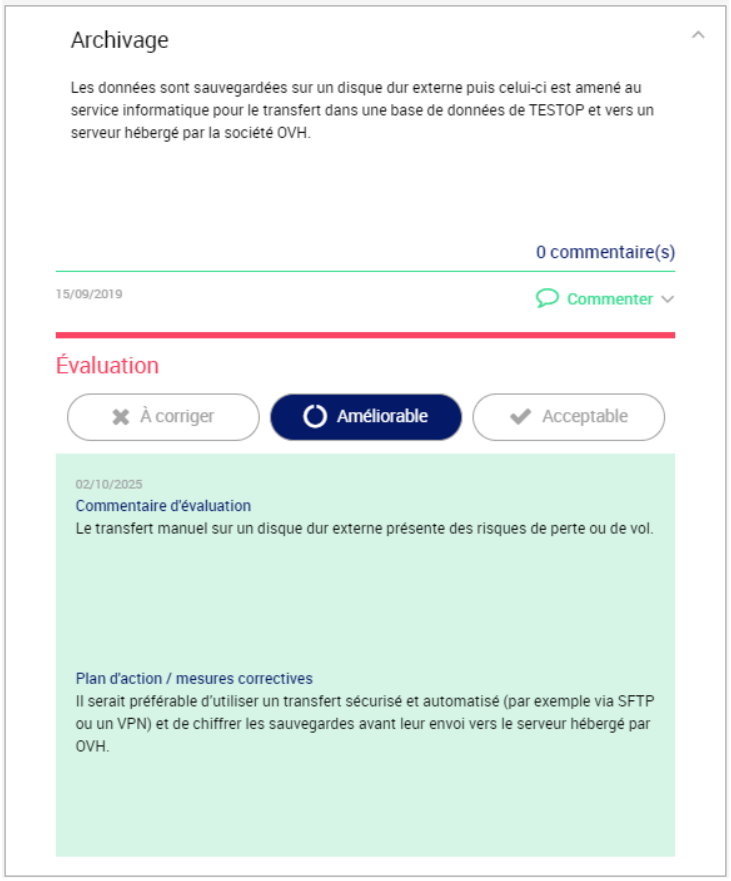
3) Pour le moment la cartographie des risques est la suivante :

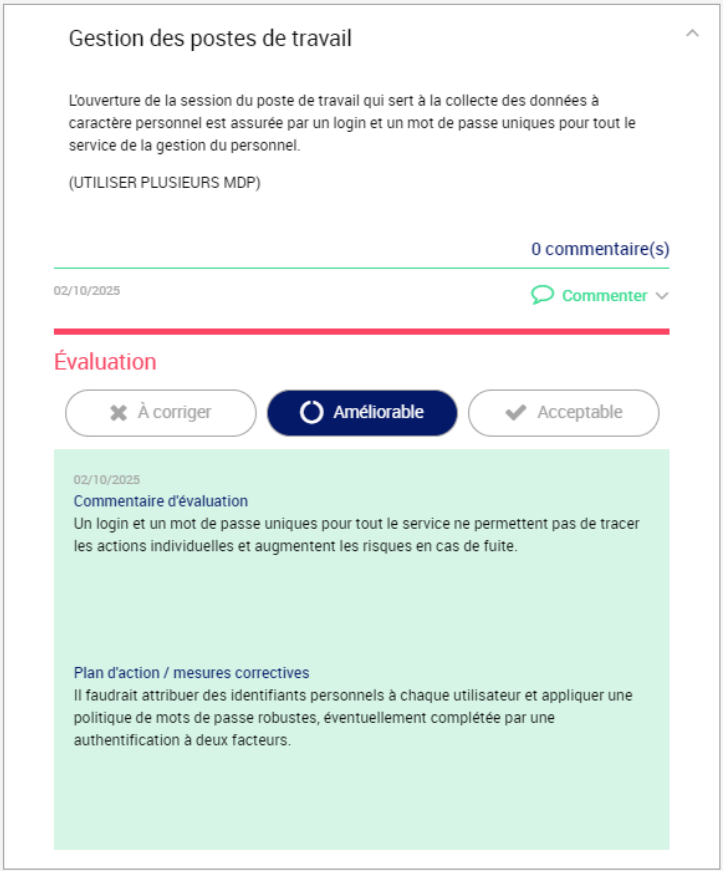


4) **MESURES EXISTANTES OU PRÉVUES :**





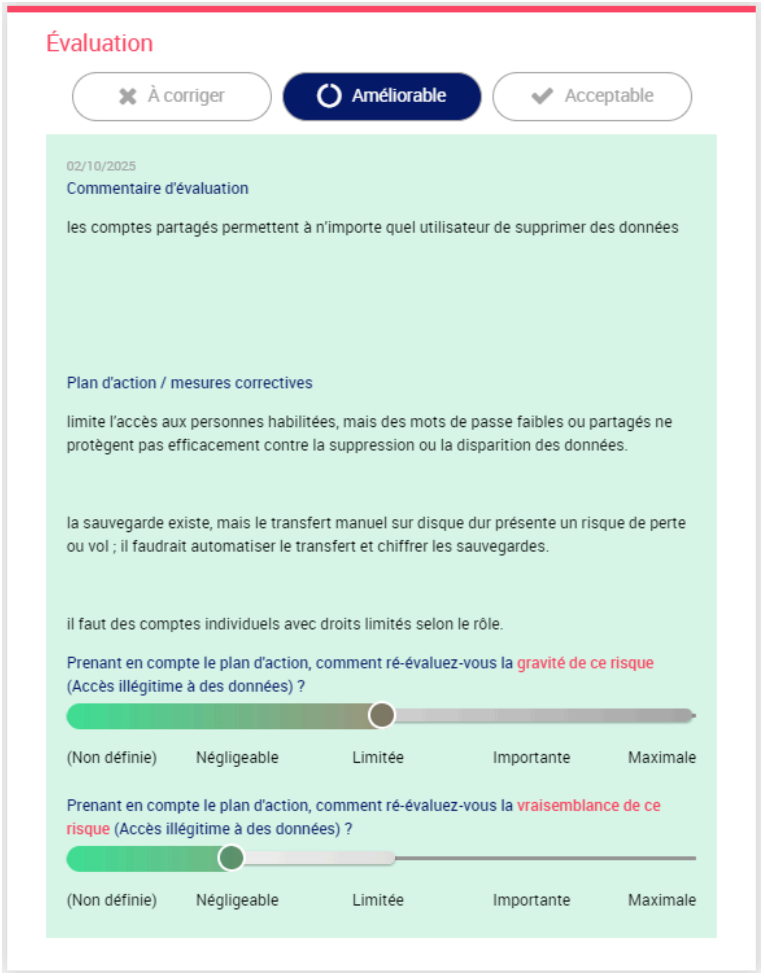

Archivage
Les données sont sauvegardées sur un disque dur externe puis celui-ci est amené au service informatique pour le transfert dans une base de données de TESTOP et vers un serveur hébergé par la société OVH.
0 commentaire(s)
15/09/2019
Commenter
Évaluation
À corriger
Améliorable
Acceptable
02/10/2025
Commentaire d'évaluation
Le transfert manuel sur un disque dur externe présente des risques de perte ou de vol.
Plan d'action / mesures correctives
Il serait préférable d'utiliser un transfert sécurisé et automatisé (par exemple via SFTP ou un VPN) et de chiffrer les sauvegardes avant leur envoi vers le serveur hébergé par OVH.


Gestion des postes de travail
L'ouverture de la session du poste de travail qui sert à la collecte des données à caractère personnel est assurée par un login et un mot de passe uniques pour tout le service de la gestion du personnel.
(UTILISER PLUSIEURS MDP)
0 commentaire(s)
02/10/2025
Commenter
Évaluation
À corriger
Améliorable
Acceptable
02/10/2025
Commentaire d'évaluation
Un login et un mot de passe uniques pour tout le service ne permettent pas de tracer les actions individuelles et augmentent les risques en cas de fuite.
Plan d'action / mesures correctives
Il faudrait attribuer des identifiants personnels à chaque utilisateur et appliquer une politique de mots de passe robustes, éventuellement complétée par une authentification à deux facteurs.

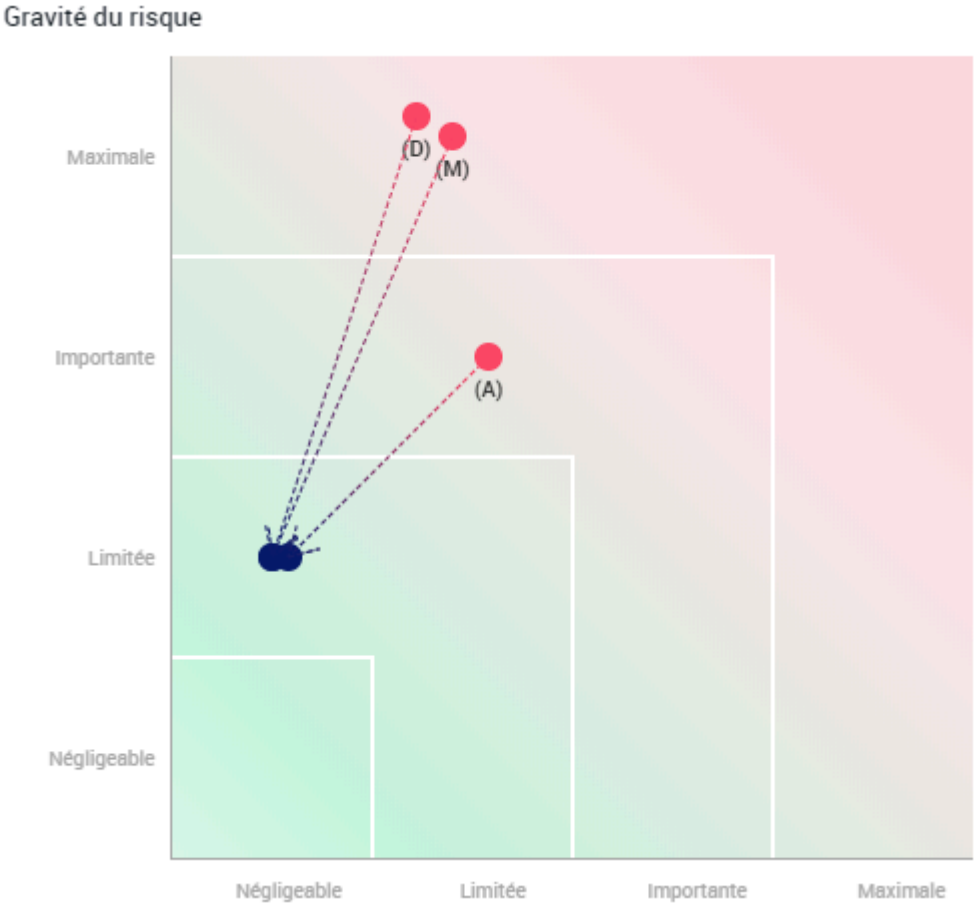
ACCÈS ILLÉGITIME À DES DONNÉES :

MODIFICATION NON DÉSIRÉES DE DONNÉES :

DISPARITION DE DONNEES :



5) Après toutes ces modifications, voici la cartographie des risques :



Nous voyons que les risques sont encore présents mais largement limités.

Exercices 2 :

1) La cartographie des traitements des données personnelles est un processus essentiel pour toute organisation souhaitant se conformer au règlement général sur la protection des données. Elle consiste à recenser, décrire et organiser l'ensemble des traitements de données personnelles effectués au sein de l'entreprise. Cette démarche permet d'avoir une vision claire et structurée des flux de données, facilitant ainsi la gestion des risques et la mise en place de mesures de sécurité appropriées.

2) Il est nécessaire de faire le registre des traitements des données à caractère personnel avant afin de ne pas oublier de risques mais surtout de pouvoir corriger ce qui doit l'être. Cela permet de recenser tous les risques et les mesures au même endroit.

Exercices 3 :

1) Lorsque l'on saisit des données personnelles (nom, email, historique d'achats…) sur castorama.fr, elles peuvent être :
   - Utilisés pour nous identifier et gérer notre compte
   - Partagé avec d'autres sociétés du groupe
   - Utilisé à des fins d'analyse ou d'études

   Les données ne restent donc pas uniquement chez Castorama, elles peuvent être partagées avec d'autres entités et utilisées pour des analyses.

2) Non, la seule lecture de l'extrait ne permet pas de dire que la confidentialité n'est pas assurée. Le texte indique que les données peuvent être partagées avec des tiers, mais il ne précisent pas comment elles sont protégées (ex : chiffrement, contrôle d'accès). Pour affirmer qu'il y a un problème de confidentialité, il faudrait connaître les mesures de sécurité mises en place par Castorama.

Exercices 4 :

1) -collecte : formulaire en ligne, cookies, carte de fidélité…
   -Stockage : bases de données, serveurs d'entreprise…
   -Diffusion : campagnes marketing, partage avec des partenaires commerciaux…

2) -Collecte et enregistrement des données.
-Conservation et organisation (bases de données)
-Analyse statistique et marketing
-Transmission à des tiers
-Suppression ou anonymisation des données

3) -Obtenir le consentement des personnes avant de collecter et d'utiliser leurs données.
-Respecter RGP
-Garantir la confidentialité, l'intégrité et la disponibilité des données.
-Permettre l'accès, la rectification et la suppression des données par les utilisateurs
-Ne collecter que les données nécessaires

4) -Amendes administratives
-Dommages et intérêts aux victimes
-perte de confiance et atteinte à la réputation de l'entreprise

Exercices 5 :

Scénarios	Sécurité	Sûreté	Justifications
L'ensemble des serveurs est hors-service à cause d'une inondation du local technique.		✅	L'inondation est un événement naturel, donc c'est une menace non intentionnelle
Les données d'un hôpital sont illisibles à la suite d'une attaque de type ransomware.	✅		L'attaque est délibérée et malveillante
L'apparence du site vitrine d'une entreprise est modifiée pendant le week-end par des personnes malveillantes.	✅		L'attaque est délibérée et malveillante
Une surcharge électrique temporaire due à des travaux réalisés dans les bâtiments de la société provoque une panne des routeurs.		✅	Il s'agit d'un incident accidentel lié à l'environnement

Exercices 6 :

Données	Caractère personnel	Justifications
Le nom de l'enseigne du magasin carrefour	Non	Ce n'est pas une personne physique mais une entreprise
L'adresse Courriel professionnelle d'un directeur des services informatiques	Oui	Elle permet d'identifier directement une personne physique
Une photo postée sur un réseau social	Oui	l'image peut permettre d'identifier la personne
Une vidéo de présentation de son parcours professionnel envoyée à une entreprise dans le cadre d'un recrutement	Oui	La vidéo peut permettre d'identifier la personne
Les coordonnées GPS de localisation d'un smartphone	Oui	Une personne qui aurait accès aux coordonnées pourrait trouver la personne
Le groupe sanguin d'un patient stocké sur le serveur de base de données de son médecin	Oui	Le groupe sanguin est forcément lié à un dossier avec le nom de la personne
Les enregistrements de vidéosurveillance d'un datacenter	Oui	L'image des personnes filmées est un élément qui permet de les identifier
Le numéro d'enregistrement au registre du commerce et des société d'une entreprise	Non	On parle ici d'une entreprise, pas d'une personne physique
Le numéro de sécurité sociale d'un salarié saisi sur la fiche d'embauche	Oui	Identifiant unique d'une personne physique.

Conclusion :

Ce tp a été un peu compliqué au début à cause de l'application un peu compliqué à comprendre sur le début mais après avoir analysé le logiciel, on découvre que c'est une application très utile pour les entreprises.